

# The number of profinite groups with a specified Sylow subgroup

Colin D. Reid

University of Newcastle

School of Mathematical and Physical Sciences

University Drive, Callaghan NSW 2308

Australia

colin@reidit.net

January 11, 2013

## Abstract

Let  $S$  be a finitely generated pro- $p$  group. Let  $\mathcal{E}_{p'}(S)$  be the class of profinite groups  $G$  that have  $S$  as a Sylow subgroup, and such that  $S$  intersects non-trivially with every non-trivial normal subgroup of  $G$ . In this paper, we investigate the question of whether or not  $\mathcal{E}_{p'}(S)$  has finitely many isomorphism classes. For instance, we give an example where  $\mathcal{E}_{p'}(S)$  contains an infinite ascending chain of soluble groups, and on the other hand show that  $\mathcal{E}_{p'}(S)$  contains only finitely many isomorphism classes in the case that  $S$  is just infinite.

*Keywords:* Profinite groups, Sylow theory

## 1 Introduction

Groups of prime power order are a pervasive feature of finite group theory. This is clearest in Sylow's theorem and more generally in the theory of fusion (also known as local analysis). The immediate goal is to understand the manner in which a  $p$ -group can be embedded in a finite group, especially with regard to the normalisers of its subgroups, as a tool for understanding finite groups by means of the  $p$ -groups contained in them. The theory of fusion in finite groups is well-developed, and in particular played a large role in the classification of finite simple groups. It has also developed into a more general theory of fusion systems of finite  $p$ -groups, which do not necessarily arise from fusion within a finite group. (See [2] for an account of this theory.)

Sylow's theorem generalises directly to profinite groups: in a profinite group  $G$ , every pro- $p$  subgroup is contained in a maximal pro- $p$  subgroup, which we call a  $p$ -Sylow subgroup, all  $p$ -Sylow subgroups are conjugate, and if  $S$  is a  $p$ -Sylow subgroup of  $G$  then  $SN/N$  is a  $p$ -Sylow subgroup of  $G/N$  for every (finite or profinite) quotient of  $G$ . In principle, the theory of fusion can be developed for profinite groups in much the same way as for finite groups. Indeed, the fact that pro- $p$  groups are generally better understood than profinite groups would suggest this as an approach for extending results from the former class to the latter. However, fusion theory is much less developed for profinite groups than for finite groups. As far as the author is aware, the first significant foray into this area was a paper by Gilotti, Ribes and Serena ([6]); since then, fusion and fusion systems in a profinite context have also been developed by Stancu and Symonds (see [12] and [14]).

A basic problem in this area is to understand the profinite groups that have a given  $p$ -Sylow subgroup  $S$ . Write  $p'$  for the set of primes other than  $p$ . Any profinite group  $G$  has a unique largest normal pro- $p'$  subgroup  $O_{p'}(G)$ , the  $p'$ -core of  $G$ . From the point of view of the associated fusion system on  $S$  (that is, the category of homomorphisms between closed subgroups of  $S$  that are induced by conjugation in  $G$ ), the  $p'$ -core plays no role, in that fusion in a  $p$ -Sylow subgroup of  $G$  is equivalent to fusion in a  $p$ -Sylow subgroup of  $G/O_{p'}(G)$ . In any case, the  $p$ -Sylow subgroups of  $G$  impose no meaningful restriction on the structure of  $O_{p'}(G)$ , for instance we could have  $G = S \times H$  where  $H$  is any pro- $p'$  group. So we are left with the following problem.

**Problem 1.** Let  $S$  be a pro- $p$  group. Let  $\mathcal{E}_{p'}(S)$  be the class of profinite groups that have  $S$  as a  $p$ -Sylow subgroup and have no non-trivial normal pro- $p'$  subgroups. Describe  $\mathcal{E}_{p'}(S)$  in terms of internal properties of  $S$ .

A natural question to ask here is the following:

**Question 2.** For which pro- $p$  groups  $S$  does  $\mathcal{E}_{p'}(S)$  contain infinitely many isomorphism classes of profinite group?

This question, and variants of it, will be the focus of this paper. For the purposes of this paper, all subgroups are required to be closed and all homomorphisms are required to be continuous, and a 'finite' class of groups is one that contains finitely many isomorphism classes of topological groups. We will concentrate on the case that  $S$  is (topologically) finitely generated, which appears to be more tractable. The following can be deduced from a theorem of Tate:

**Lemma 1.1.** *Let  $S$  be a finitely generated pro- $p$  group. Then every group in  $\mathcal{E}_{p'}(S)$  is virtually pro- $p$ .*

If  $G \in \mathcal{E}_{p'}(S)$ , then there is a subgroup  $P$  of  $S$  which is open and normal in  $G$ ; now  $P$  is also finitely generated, so  $\Phi(P)$  is also open in  $G$ . It follows from some basic extension

theory that  $G$  is determined as an element of  $\mathcal{E}_{p'}(S)$  by the quotient  $G/P$  together with its action on  $P/\Phi(P)$ :

**Theorem 1.2.** *Let  $P$  be a finitely generated pro- $p$  group, and let  $K$  be a finite group. Suppose the extensions*

$$1 \longrightarrow P \longrightarrow G \longrightarrow K \longrightarrow 1$$

and

$$1 \longrightarrow P \longrightarrow G^* \longrightarrow K \longrightarrow 1$$

admit a common restriction

$$1 \longrightarrow P \longrightarrow S \longrightarrow T \longrightarrow 1$$

where  $T$  is a  $p$ -Sylow subgroup of  $K$ , and the action of  $K$  on  $P/\Phi(P)$  is the same in both extensions.

Then the extensions are equivalent, and hence  $G \cong G^*$ .

**Corollary 1.3.** *Let  $S$  be a finitely generated pro- $p$  group. Then for all  $n$ , the number of isomorphism types of profinite group  $G$  having  $S$  as a Sylow subgroup of index at most  $n$  is finite. In particular,  $\mathcal{E}_{p'}(S)$  is at most countably infinite, and  $\mathcal{E}_{p'}(S)$  is finite if and only if there is an overall bound on  $|G : S|$  for all  $G \in \mathcal{E}_{p'}(S)$ .*

So Question 2 is equivalent to asking whether there is a bound on  $|G : S|$  (or equivalently on  $|G : \mathcal{O}_p(G)|$ , or on  $|G : \Phi(\mathcal{O}_p(G))|$ ).

It is also of interest to consider two more restricted classes of  $p'$ -embeddings:

**Definition 1.4.** Let  $G$  be a profinite group. A *component* of  $G$  is a subnormal subgroup  $Q$  such that  $Q$  is perfect and  $Q/Z(Q)$  is simple. (Note that these conditions ensure that  $Q$  is finite.) Define the *layer*  $E(G)$  of  $G$  to be the closed subgroup of  $G$  generated by the components of  $G$ . Given a pro- $p$  group  $S$ , define  $\mathcal{E}_{p'}^{\text{LF}}(S)$  to be the class of groups  $G \in \mathcal{E}_{p'}(S)$  such that  $E(G) = 1$ . Define  $\mathcal{E}_{p'}^{\text{sep}}(S)$  to be the class of groups in  $\mathcal{E}_{p'}(S)$  that are  $p$ -separable, that is, which have no non-abelian composition factors of order divisible by  $p$ .

The *pro-Fitting subgroup*  $F(G)$  of  $G$  is the unique largest normal pronilpotent subgroup of  $G$ . The *generalised pro-Fitting subgroup*  $F^*(G)$  of  $G$  is given by  $F^*(G) = F(G)E(G)$ .

In a virtually pronilpotent group, the generalised pro-Fitting subgroup contains its own centraliser (see [9]), so if  $G \in \mathcal{E}_{p'}^{\text{LF}}(S)$  for a finitely generated pro- $p$  group  $S$ , then  $\mathcal{O}_p(G)$  contains its own centraliser in  $G$ , and indeed  $G/\mathcal{O}_p(G)$  acts faithfully on  $\mathcal{O}_p(G)/\Phi(\mathcal{O}_p(G))$ . So if  $S$  is finite, or more generally if  $S$  has finite subgroup rank, then we obtain a bound on  $|G/\mathcal{O}_p(G)|$ , so  $\mathcal{E}_{p'}^{\text{LF}}(S)$  is finite. Even in this case it can happen

that  $\mathcal{E}_{p'}(S)$  is infinite: for instance,  $S$  may be the  $p$ -Sylow subgroup of infinitely many finite simple groups. More interesting is the case when  $\mathcal{E}_{p'}^{\text{LF}}(S)$  or  $\mathcal{E}_{p'}^{\text{sep}}(S)$  is infinite. Consider for instance the following:

**Proposition 1.5.** *Let  $p$  and  $q$  be distinct primes. Then there is a 2-generator metabelian pro- $p$  group  $S$  and an infinite ascending chain*

$$S < G_0 < G_1 < G_2 < \dots$$

*of profinite groups, each open in the next, with the following properties:*

*the union  $G = \bigcup_{i \geq 0} G_i$  is a soluble group of derived length 3, and  $G = SQ$  where  $Q$  is a countably infinite discrete elementary abelian  $q$ -group;*

*for all  $i \geq 0$ ,  $O_{p'}(G_i) = 1$ , so  $G_i \in \mathcal{E}_{p'}^{\text{sep}}(S)$ ;*

*the fusion systems  $\mathcal{F}_{G_i}(S)$  are pairwise non-isomorphic; indeed, the fusion of conjugacy classes of  $S$  in  $G_i$  and  $G_j$  is inequivalent for all  $i \neq j$ .*

Nevertheless, there are significant restrictions on the structure of  $p'$ -embeddings of 2-generator pro- $p$  groups (See Theorem 6.2 below). The reason for this is the role played normal subgroups  $P$  of a pro- $p$  group  $S$  that are not contained in  $\Phi(S)$ , and in the 2-generator case,  $P \not\leq \Phi(S)$  implies  $S/P$  is cyclic (in particular,  $P \geq S'$ ). Indeed, for groups  $S$  such that  $P \not\leq \Phi(S)$  for only finitely many normal subgroups  $P$ , we obtain the following:

**Theorem 1.6.** *Let  $S$  be an infinite finitely generated pro- $p$  group. Let  $\mathcal{K}$  be the set of open normal subgroups of  $S$  that are not contained in  $\Phi(S)$ . Suppose that  $\mathcal{K}$  is finite. Then  $\mathcal{E}_{p'}(S) = \mathcal{E}_{p'}^{\text{LF}}(S)$  and  $\mathcal{E}_{p'}^{\text{sep}}(S)$  is finite. If in addition  $|S : S^{(n)}|$  is finite for all  $n$ , then  $\mathcal{E}_{p'}(S)$  is finite.*

The hypotheses of Theorem 1.6 are immediately satisfied if  $S$  is generated by 2 elements and  $|S : S^{(n)}|$  is finite for all  $n$ , because the order of a cyclic quotient is at most  $|S : S'|$ . The hypotheses of Theorem 1.6 are also satisfied by all just infinite pro- $p$  groups of infinite subgroup rank. As a result we obtain the following:

**Theorem 1.7.** *Let  $S$  be a just infinite pro- $p$  group. Then  $\mathcal{E}_{p'}(S)$  is finite. In other words, only finitely many just infinite groups have  $S$  as a Sylow subgroup.*

In general, for a given finitely generated pro- $p$  group  $S$ , the question of whether  $\mathcal{E}_{p'}(S)$ ,  $\mathcal{E}_{p'}^{\text{LF}}(S)$  or  $\mathcal{E}_{p'}^{\text{sep}}(S)$  is finite reduces to considering  $p'$ -embeddings of more restricted types (see Theorem 5.2). We also obtain several restrictions (Theorem 8.3) on the structure of groups in  $\mathcal{E}_{p'}(S)$  in the case that  $S$  is weakly regular, that is,  $S$  does not have a quotient isomorphic to  $C_p \wr C_p$ . This class of pro- $p$  groups includes for instance all nilpotent pro- $p$  groups of class less than  $p$  and all powerful pro- $p$  groups. It is not known if there are any finitely generated weakly regular pro- $p$  groups  $S$  for which  $\mathcal{E}_{p'}^{\text{LF}}(S)$  is infinite.

## 2 Preliminaries

We gather here some basic facts and definitions we will need about finite and profinite groups.

**Definition 2.1.** Let  $G$  be a profinite group. Define  $d(G)$  to be the size of the smallest subset  $X$  of  $G$  such that  $G = \overline{\langle X \rangle}$ . Say  $G$  is  $n$ -generated if  $d(G) \leq n$ .

Define  $G'$  to be the closed commutator subgroup  $\overline{[G, G]}$ , and define  $G^{(n)}$  inductively by  $G^{(0)} = G$  and  $G^{(n+1)} = (G^{(n)})'$ . Write  $G^n$  for the smallest closed subgroup of  $G$  containing all  $n$ -th powers in  $G$ .

Given a prime (or set of primes)  $p$ , the  $p$ -core  $O_p(G)$  is the largest normal pro- $p$  subgroup of  $G$ , and the  $p$ -residual  $O^p(G)$  is the smallest normal subgroup of  $G$  such that  $G/O^p(G)$  is a pro- $p$  group.

**Lemma 2.2.** Let  $G$  be a profinite group and let  $\mathcal{Q}$  be a set of components of  $G$ . Then  $K = \overline{\langle \mathcal{Q} \rangle}$  is a central product of  $\mathcal{Q}$  and no proper subset of  $\mathcal{Q}$  suffices to generate  $K$  topologically. Every component of  $G$  is contained in a finite normal subgroup of  $G$ .

*Proof.* See [9] Proposition 2.8. □

**Lemma 2.3.** Let  $P$  be a finitely generated pro- $p$  group and let  $G = P \rtimes H$  be a profinite group such that  $C_H(P) = 1$ .

(i) Suppose there is an  $H$ -invariant series

$$P = P_1 \geq P_2 \geq \dots$$

of normal subgroups of  $P$ , such that  $\bigcap P_i = 1$ , and such that  $[P_i, H] \leq P_{i+1}$  for each  $i$ . Then  $H$  is a pro- $p$  group.

(ii) Define the characteristic series  $P_i$  by  $P_1 = P$ , and thereafter  $P_{i+1} = [P, P_i]P_i^p$ . Suppose  $H$  acts trivially on  $P/\Phi(P)$ . Then  $H$  acts trivially on  $P_i/P_{i+1}$  for all  $i$ . In particular,  $H$  is a pro- $p$  group.

(iii) Suppose  $P$  is finite and abelian, and  $H$  is a  $p'$ -group. Then  $P = [P, H] \times C_P(H)$ .

*Proof.* For parts (i) and (ii) see [7] Exercise 2.1 (2); the generalisation to profinite groups is immediate. For part (iii) see [1] Proposition 24.6. □

**Lemma 2.4.** Let  $G$  be a profinite group that is virtually pronilpotent. Then  $C_G(F^*(G)) = Z(F(G))$ .

*Proof.* This is a special case of [9], Theorem 1.7. □

**Corollary 2.5.** *Let  $S$  be a finitely generated pro- $p$  group, let  $G \in \mathcal{E}_{p'}^{\text{LF}}(S)$  and let  $P = \text{O}_p(G)$ . Then  $G/P$  acts faithfully on  $P/\Phi(P)$ . As a result, we have  $H \in \mathcal{E}_{p'}^{\text{LF}}(S)$  for all closed subgroups  $H$  of  $G$  containing  $S$ .*

*Proof.* By Lemma 2.4, we have  $C_G(P) \leq P$ . By Lemma 2.3, the section  $C_G(P/\Phi(P))/C_G(P)$  is a pro- $p$  group, so  $C_G(P/\Phi(P))$  is a pro- $p$  group; since  $\Phi(P) \geq P'$ , we have  $P \leq C_G(P/\Phi(P))$ . But  $P$  is the largest normal pro- $p$  subgroup of  $G$ , so in fact  $P = C_G(P/\Phi(P))$ .

Now let  $H$  be a subgroup of  $G$  containing  $S$ . Clearly  $S$  is a  $p$ -Sylow subgroup of  $H$ . We have  $C_H(\text{O}_p(H)) \leq C_H(P) \leq P$ , since  $P$  is a normal pro- $p$  subgroup of  $H$ . This ensures that  $\text{E}(H)$  and  $\text{O}_{p'}(H)$  are both trivial. Thus  $H \in \mathcal{E}_{p'}^{\text{LF}}(S)$ .  $\square$

**Definition 2.6.** Let  $P$  be a finite  $p$ -group. A characteristic subgroup  $K$  of  $P$  is *critical* if  $[P, K]\Phi(K) \leq Z(K)$  and  $C_P(K) = Z(K)$ .

**Theorem 2.7** (Thompson, [4] Chapter II, Lemma 8.2). *Let  $P$  be a finite  $p$ -group. Then  $P$  has a critical subgroup. If  $K$  is a critical subgroup of  $P$ , then the kernel of the induced homomorphism  $\text{Aut}(P) \rightarrow \text{Aut}(K)$  is a  $p$ -group.*

### 3 Control of $p$ -transfer in profinite groups

An important notion in finite group theory is the *transfer map*, which is a homomorphism that is defined from a finite group to any of its abelian sections. We will not be using the transfer map directly, but we will be using the closely related notion of control of transfer, and more precisely control of  $p$ -transfer. Control of transfer is a concept that behaves well in the class of profinite groups; see for instance [6]. (Note however that our definition of which subgroup controls transfer is slightly different to that used in [6].)

**Definition 3.1.** Let  $G$  be a profinite group, let  $H$  be a subgroup, and let  $H \leq K \leq G$ . Say  $K$  *controls transfer* from  $G$  to  $H$  if  $G' \cap H = K' \cap H$ . In the special case that  $H$  is a  $p$ -Sylow subgroup of  $G$ , then say  $K$  *controls  $p$ -transfer* in  $G$ . There is a potential ambiguity in saying that  $K$  controls  $p$ -transfer in  $G$  without specifying the Sylow subgroup, but since all Sylow subgroups of  $G$  contained in  $K$  are conjugate in  $K$ , the choice of Sylow subgroup is immaterial in practice.

The theorem below is an interpretation essentially due to Gagola and Isaacs ([5]) of a theorem of Tate ([15]). Both [15] and [5] state the result for finite groups, but the generalisation to profinite groups is immediate.

**Theorem 3.2** (Tate). *Let  $G$  be a (pro-)finite group, let  $S$  be a  $p$ -Sylow subgroup of  $G$ , and let  $S \leq K \leq G$ . The following are equivalent:*

- (i)  $G' \cap S = K' \cap S$ ;
- (ii)  $(G'G^p) \cap S = (K'K^p) \cap S$ ;
- (iii)  $(G'\mathrm{O}^p(G)) \cap S = (K'\mathrm{O}^p(K)) \cap S$ ;
- (iv)  $\mathrm{O}^p(G) \cap S = \mathrm{O}^p(K) \cap S$ .

From now on, the statement ‘ $K$  controls  $p$ -transfer in  $G$ ’ will be taken to mean any of the four equations above interchangeably.

In a profinite group  $G$ , a *normal  $p$ -complement* is a (necessarily unique) normal subgroup  $N$  such that  $G = SN$  and  $S \cap N = 1$ , where  $S$  is a  $p$ -Sylow subgroup of  $G$ . Theorem 3.2 has some immediate consequences for normal  $p$ -complements in normal subgroups of (pro-)finite groups (indeed, this was the original motivation of Tate’s result in the finite context).

**Corollary 3.3.** *Let  $G$  be a profinite group, and let  $S \in \mathrm{Syl}_p(G)$ .*

- (i) *Let  $M$  be a normal subgroup of  $G$  such that  $S \cap M \leq \Phi(S)$ . Then  $SM$  has a normal  $p$ -complement, and  $\mathrm{O}_{p'}(G/M) = \mathrm{O}_{p'}(G)M/M$ .*
- (ii) *Let  $M$  and  $N$  be normal subgroups of  $G$  such that  $S \cap M \leq \Phi(S)N$ . Then  $MN/N$  has a normal  $p$ -complement.*

*Proof.* (i) For any normal subgroup  $M$  of  $G$ , we have  $(SM)'(SM)^p = \Phi(S)M$ . The condition  $S \cap M \leq \Phi(S)$  then implies

$$((SM)'(SM)^p) \cap S = \Phi(S)M \cap S = \Phi(S) = S'S^p.$$

Hence by Theorem 3.2 we have  $\mathrm{O}^p(SM) \cap S = \mathrm{O}^p(S) \cap S = 1$ , in other words  $\mathrm{O}^p(SM)$  is the normal  $p$ -complement of  $SM$ . Note that  $\mathrm{O}^p(SM)$  is also a normal  $p$ -complement in  $M$ .

For the final assertion, let  $O$  be the lift of  $\mathrm{O}_{p'}(G/M)$  to  $G$ . It is clear that  $O \geq \mathrm{O}_{p'}(G)M$ . On the other hand,  $S \cap O = S \cap M \leq \Phi(S)$ , so  $O$  has a normal  $p$ -complement  $K$ , by the same argument as for  $M$ . Since  $M$  contains a  $p$ -Sylow subgroup of  $O$ , we have  $O = KM$ ; since  $K$  is a normal pro- $p'$  subgroup of  $G$ , we have  $K \leq \mathrm{O}_{p'}(G)$ , so  $O = \mathrm{O}_{p'}(G)M$ .

(ii)  $MN/N$  is a normal subgroup of  $G/N$ , and  $\Phi(S/N) = \Phi(S)N/N$  contains  $(M \cap S)N/N$ . The result follows by part (i) applied to  $G/N$ .  $\square$

*Proof of Lemma 1.1.* Since  $\Phi(S)$  is open in  $S$ , there is some open normal subgroup  $N$  of  $G$  such that  $S \cap N \leq \Phi(S)$ . By Corollary 3.3,  $N/\mathrm{O}_{p'}(N)$  is a pro- $p$  group, so  $G/\mathrm{O}_{p'}(N)$  is virtually pro- $p$ . Now  $\mathrm{O}_{p'}(N) \leq \mathrm{O}_{p'}(G)$ , so  $G/\mathrm{O}_{p'}(G)$  is an image of  $G/\mathrm{O}_{p'}(N)$ ; hence  $G/\mathrm{O}_{p'}(G)$  is virtually pro- $p$ .  $\square$

It is worth noting in particular a sufficient condition under which every  $p'$ -embedding is layer-free.

**Corollary 3.4.** *Let  $S$  be a finitely generated pro- $p$  group and let  $G \in \mathcal{E}_{p'}(S)$ . Suppose that  $\Phi(S)$  contains every finite normal subgroup of  $S$ . Then  $E(G) = 1$ .*

*Proof.* Certainly  $E(G)$  is finite, since  $G$  is virtually pro- $p$  by Lemma 1.1, so  $E(G) \cap S$  is a finite normal subgroup of  $S$ . Additionally,  $p$  divides the order of every component of  $G$ , since  $O_{p'}(G) = 1$ . But  $E(G) \cap S \leq \Phi(S)$ , so  $E(G)$  has a normal  $p$ -complement. Hence  $E(G) = 1$ .  $\square$

**Definition 3.5.** Let  $S$  be a finitely-generated pro- $p$  group and let  $G$  be a  $p'$ -embedding of  $S$ . Say  $G$  is *Frattini* if  $O_p(G) \leq \Phi(S)$ , or more generally, say  $G$  is *quasi-Frattini* if  $O_p(G) \cap \Phi(S)$  is normal in  $G$ . Say  $G$  is *standard* if  $O_p(G) \cap \Phi(S)$  is not normal in  $G$ .

Given a profinite group  $G$ , define the  $p$ -layer  $E_p(G)$  to be the set of components of  $G$  of order divisible by  $p$ . (Note that if a quasisimple group  $Q$  is of order divisible by  $p$ , then the simple quotient  $Q/Z(Q)$  is also of order divisible by  $p$ .)

**Lemma 3.6.** *Let  $G$  be a (topological) group and let  $\alpha$  be an automorphism of  $G$  (as a topological group) that acts trivially on  $G/Z(G)$ . Then  $\alpha$  acts trivially on  $G'$ . In particular, if  $G$  is (topologically) perfect then  $\text{Aut}(G)$  acts faithfully on  $G/Z(G)$ .*

*Proof.* Let  $\alpha$  be an automorphism of  $G$  and write  $[\alpha, x]$  for  $x\alpha(x^{-1})$ . Suppose  $[\alpha, x] \in Z(G)$  for all  $x \in G$ . Then for all  $x, y \in G$ , we have the following:

$$\begin{aligned} \alpha([x, y]) &= [\alpha(x), \alpha(y)] = \alpha(x)\alpha(y)\alpha(x^{-1})\alpha(y^{-1}) = [\alpha, x]^{-1}x^{-1}[\alpha, y]^{-1}y^{-1}x[\alpha, x]y[\alpha, y] \\ &= xyx^{-1}y^{-1} = [x, y], \end{aligned}$$

so  $\alpha$  fixes every commutator in  $G$ . Since  $G'$  is generated topologically by the commutators in  $G$ , it follows that the action of  $\alpha$  on  $G'$  is trivial.  $\square$

**Lemma 3.7.** *Let  $S$  be a non-trivial finitely generated pro- $p$  group and let  $G \in \mathcal{E}_{p'}(S)$  be quasi-Frattini. Then  $S/O_p(G)$  acts faithfully on  $E_p(G/O_p(G))$ . In particular,  $G$  is  $p$ -separable if and only if  $S \trianglelefteq G$ . If  $G \in \mathcal{E}_{p'}(S)$  is Frattini, then  $G/O_p(G)$  acts faithfully on  $E_p(G/O_p(G))$ .*

*Proof.* Let  $K = O_p(G) \cap \Phi(S)$  and let  $E = E_p(G/O_p(G))$ . By Corollary 3.3 (i),  $O_{p'}(G/K) = 1$ . Thus  $F^*(G/K)$  is generated by  $O_p(G)/K$  together with the components of  $G/K$ , and all components of  $G/K$  have order divisible by  $p$ . The centraliser of  $F^*(G/K)$  inside  $G/K$  is  $Z(F^*(G/K))$ , which is a subgroup of  $O_p(G/K)$  since  $O_{p'}(G/K) = 1$ . The action of  $S$  on  $O_p(G)/K$  is trivial, since  $O_p(G)/K$  corresponds to  $O_p(G)\Phi(S)/\Phi(S)$ , which is a central factor of  $S$  as  $\Phi(S) \geq [S, S]$ . Thus the kernel of the action of  $S/K$  on  $E_p(G/K)$  is contained in  $O_p(G)$ . Now  $E$  corresponds to a quotient of



the perfect group  $E_p(G/K)$  by a central subgroup, so  $S/O_p(G)$  acts faithfully on  $E$  by Lemma 3.6. If  $S$  is not normal in  $G$ , then  $S/O_p(G)$  is non-trivial, so  $E$  is also non-trivial, so  $G$  is not  $p$ -separable.

If  $O_p(G) \leq \Phi(S)$ , we have  $K = O_p(G)$ , so  $F^*(G/K) = E_p(G/K) = E$ , and  $Z(E_p(G/K)) = 1$  so we have a faithful action of  $G/O_p(G)$  on  $E$ .  $\square$

## 4 Extension theory

Given a group  $G$  acting on an abelian group  $M$ , write  $H^n(G, M)$  for the  $n$ -th cohomology group of  $G$  on  $M$ .

**Proposition 4.1.** *Let  $G$  be a finite group, and let  $M$  be an abelian finite group on which  $G$  acts. Given an extension*

$$\mathcal{E} = \{ 1 \longrightarrow M \xrightarrow{\alpha} E \xrightarrow{\pi} G \longrightarrow 1 \}$$

*of  $M$  by  $G$ , obtain  $t_{\mathcal{E}}$  as follows:*

*Let  $\tau$  be any function from  $G$  to  $E$  such that  $\pi\tau = \text{id}_G$ . Let  $f : G \times G \rightarrow M$  be the function determined by the equation  $\tau(x)\tau(y) = \tau(xy)\alpha(f(x, y))$ . Let  $t_{\mathcal{E}}$  be the equivalence class of  $f$  modulo 2-coboundaries.*

*Then:*

- (i)  $f$  is a 2-cocycle, any choice of  $\tau$  gives the same  $t_{\mathcal{E}}$ , and  $t_{\mathcal{E}}$  depends only on the equivalence class of the extension  $\mathcal{E}$ ;*
- (ii) the map  $\mathcal{E} \mapsto t_{\mathcal{E}}$  defines a bijection from the set of equivalence classes of extensions of  $M$  by  $G$  to  $H^2(G, M)$ ;*
- (iii)  $\mathcal{E}$  splits if and only if  $t_{\mathcal{E}} = 0$ .*

*Proof.* See [16], Lemmas 6.2.1. and 6.2.2. (In fact, [16] gives a proof for profinite groups in the context of profinite cohomology.)  $\square$

**Proposition 4.2.** *Let  $M$  be a finite abelian group, and let  $G$  be a finite group acting on  $M$ . Suppose  $H$  is a subgroup of  $G$  for which  $|G : H|$  is coprime to  $|M|$ . Then for  $n > 0$ , the restriction map  $H^n(G, M) \rightarrow H^n(H, M)$  is injective.*

*Proof.* See [3], Proposition 4.2.5.  $\square$

*Proof of Theorem 1.2.* We may regard  $P$  as an open subgroup of  $S$ , and  $S$  as a  $p$ -Sylow subgroup of both  $G$  and  $G^*$ . Define subgroups  $P_i$  of  $P$  by  $P_1 = P$ , and thereafter  $P_{i+1} = [P_i, P]P_i^p$ . Then  $P_i$  is an open characteristic subgroup of  $P$  for all  $i$ . Set  $G_i = G/P_i$ , set

$G_i^* = G^*/P_i$ , and set  $M_i = P_i/P_{i+1}$ . Then for  $i \geq 1$ , we have extensions  $\mathcal{E}_i$  and  $\mathcal{E}_i^*$  of finite groups given by

$$\mathcal{E}_i = \{ 1 \longrightarrow M_i \longrightarrow G_{i+1} \longrightarrow G_i \longrightarrow 1 \}$$

$$\mathcal{E}_i^* = \{ 1 \longrightarrow M_i \longrightarrow G_{i+1}^* \longrightarrow G_i^* \longrightarrow 1 \}$$

and by an inverse limit argument, it suffices to prove that these extensions are equivalent for all  $i$ . By induction, we may assume that we have an isomorphism  $\theta$  between  $G_i$  and  $G_i^*$ ; furthermore, the actions of  $G_i$  and  $G_i^*$  on  $P_i/P_{i+1}$  are determined by the action of  $K$  on  $P_i/P_{i+1}$ , which is in turn determined by the action of  $K$  on  $P/\Phi(P)$ , by Lemma 2.3 (ii). Hence  $\theta$  induces an isomorphism from  $M_i$  as a  $G_i$ -module to  $M_i$  as a  $G_i^*$ -module. Now by Proposition 4.1, the extensions  $\mathcal{E}_i$  and  $\mathcal{E}_i^*$  are both associated in a natural way to elements  $t$  and  $t^*$  say of  $H^2(G_i, M_i)$ , and the extensions are equivalent if and only if  $t = t^*$ . However, both extensions have the common restriction

$$1 \longrightarrow M_i \longrightarrow S_{i+1} \longrightarrow S_i \longrightarrow 1 ,$$

where  $S_i = S/P_i$ . This corresponds to the condition that  $t^\rho = (t^*)^\rho$ , where  $H^2(G_i, M_i) \xrightarrow{\rho} H^2(S_i, M_i)$  is the natural restriction map. But  $S_i$  is a  $p$ -Sylow subgroup of  $G_i$  and  $M_i$  is a  $p$ -group, so by Proposition 4.2,  $\rho$  is injective. Hence  $t = t^*$  and so  $\mathcal{E}_i$  and  $\mathcal{E}_i^*$  are equivalent.  $\square$

Corollary 1.3 is immediate, given the fact that a finitely generated pro- $p$  group has only finitely many (normal) subgroups of any given finite index.

## 5 The critical cases

In this section, we establish ‘critical’ subclasses of  $\mathcal{E}_{p'}(S)$ ,  $\mathcal{E}_{p'}^{\text{LF}}(S)$  and  $\mathcal{E}_{p'}^{\text{sep}}(S)$  with more restricted structure, such that for a fixed finitely generated pro- $p$  group  $S$ , the class  $\mathcal{E}_{p'}(S)$ ,  $\mathcal{E}_{p'}^{\text{LF}}(S)$  or  $\mathcal{E}_{p'}^{\text{sep}}(S)$  is infinite if and only if the corresponding critical subclass is infinite.

**Definition 5.1.** Let  $G$  be a  $p'$ -embedding of the finitely generated pro- $p$  group  $S$  and write  $P = O_p(G)$ . Define the subclasses  $\mathcal{C}_{p'}^{\text{ab}}(S)$ ,  $\mathcal{C}_{p'}^{\text{crit}}(S)$ ,  $\mathcal{C}_{p'}^{\text{LF}}(S)$  and  $\mathcal{C}_{p'}^{\text{L}}(S)$  of  $\mathcal{E}_{p'}(S)$  respectively as follows:

Let  $G \in \mathcal{C}_{p'}^{\text{ab}}(S)$  if  $G = SH$  such that  $H$  is a non-trivial finite elementary abelian  $q$ -group (for  $q$  a prime distinct from  $p$ ),  $HP/P$  is a minimal normal subgroup of  $G/P$ ,  $G = O^q(G)$  and  $N_G(P \cap \Phi(S)) = S$ .

Let  $G \in \mathcal{C}_{p'}^{\text{crit}}(S)$  if  $G = SH$  such that  $H$  is a non-abelian finite  $q$ -group (for  $q$  a prime distinct from  $p$ ) that has no proper critical subgroups in the sense of Thompson (in

particular,  $H$  is critical in itself, so  $\Phi(H) \leq Z(H)$ ,  $HP/Z(H)P$  is a chief factor of  $G$ ,  $G = O^q(G)$  and  $N_G(P \cap \Phi(S)) \leq SZ(H)$ . Define  $\mathcal{C}_{p'}^{\text{sep}}(S) := \mathcal{C}_{p'}^{\text{ab}}(S) \cup \mathcal{C}_{p'}^{\text{crit}}(S)$ .

Let  $G \in \mathcal{C}_{p'}^{\text{LF}}(S)$  if  $E(G) = 1$  and  $G = SQ$  such that  $Q \geq P$  and  $Q/P$  is the normal closure of a component of  $G/P$  of order divisible by  $p$ .

Let  $G \in \mathcal{C}_{p'}^{\text{L}}(S)$  if  $G = SQ$  such that  $Q$  is the normal closure of a component of  $G$ . (Here the component is necessarily of order divisible by  $p$ .)

**Theorem 5.2.** *Let  $S$  be a finitely generated pro- $p$  group.*

- (i) *If  $\mathcal{C}_{p'}^{\text{sep}}(S)$  is finite then  $\mathcal{E}_{p'}^{\text{sep}}(S)$  is finite.*
- (ii) *If  $\mathcal{C}_{p'}^{\text{sep}}(S)$  and  $\mathcal{C}_{p'}^{\text{LF}}(S)$  are finite then  $\mathcal{E}_{p'}^{\text{LF}}(S)$  is finite.*
- (iii) *If  $\mathcal{C}_{p'}^{\text{sep}}(S)$ ,  $\mathcal{C}_{p'}^{\text{LF}}(S)$  and  $\mathcal{C}_{p'}^{\text{L}}(S)$  are finite then  $\mathcal{E}_{p'}(S)$  is finite.*

**Definition 5.3.** Let  $S$  be a finitely-generated pro- $p$  group. Define the invariant  $d_f(S)$  to be the maximum value of  $\log_p |K\Phi(S) : \Phi(S)|$  as  $K$  ranges over the finite normal subgroups of  $S$ . For instance,  $d_f(S) = d(S)$  if and only if  $S$  is finite, while  $d_f(S) = 0$  if and only if all finite normal subgroups of  $S$  are contained in  $\Phi(S)$ .

**Lemma 5.4.** *Let  $G$  be a profinite group with a finitely-generated  $p$ -Sylow subgroup  $S$ . Let  $\mathcal{X}$  be a set of finite normal subgroups of  $G$  and let  $H = \overline{\langle \mathcal{X} \rangle}$ . Then there is a subset  $\mathcal{K}$  of  $\mathcal{X}$  such that  $|\mathcal{K}| \leq \log_p |H\Phi(S) : \Phi(S)|$  and such that  $H/\langle \mathcal{K} \rangle$  has a normal  $p$ -complement.*

*In particular, if  $\Omega$  is the set of components of  $G$  of order divisible by  $p$ , then  $S$  has at most  $d_f(S)$  orbits on  $\Omega$  (acting by conjugation).*

*Proof.* Given a normal subgroup  $N$  of  $G$ , write  $V_S(N) = (N \cap S)\Phi(S)/\Phi(S)$ , regarded as a subspace of  $S/\Phi(S) \cong (\mathbb{F}_p)^{d(S)}$ . Since  $H$  is generated by  $\mathcal{X}$ , there are  $H_1, \dots, H_k \in \mathcal{X}$  such that

$$V_S(H) = V_S(H_1) + \dots + V_S(H_k),$$

and such that  $k \leq \dim(V_S(H)) = \log_p |H\Phi(S) : \Phi(S)|$ . Now set  $\mathcal{K} = \{H_1, \dots, H_k\}$  and let  $K = \langle \mathcal{K} \rangle$ ; then clearly

$$\Phi(S)(H \cap S) = \Phi(S)(K \cap S),$$

so  $H/K$  has a normal  $p$ -complement by Corollary 3.3 (ii).

For the final assertion, let  $H = \langle \Omega \rangle$ . Without loss of generality, we may assume  $G = SH$ ; as  $H$  is a central product of the elements of  $\Omega$ , the  $S$ -orbits on  $\Omega$  are the same as  $G$ -orbits. Indeed we have  $H = \langle \mathcal{X} \rangle$ , where  $\mathcal{X}$  consists of the normal subgroups of  $G$  formed by taking the product of the  $S$ -conjugates of a single element of  $\Omega$ . Since no element of  $\mathcal{X}$  is redundant in generating  $H$  and  $H$  has no  $p$ -separable images, we conclude that  $|\mathcal{X}| \leq d_f(S)$ , so there are at most  $d_f(S)$  orbits of  $S$  on  $\Omega$ .  $\square$

**Lemma 5.5.** *Let  $P$  be a finite abelian  $p$ -group. Write  $\Omega_i(P)$  for the group of elements of  $P$  of order dividing  $p^i$ . Let  $\alpha$  be a non-trivial automorphism of  $P$  of order coprime to  $p$ . Then  $\alpha$  induces a non-trivial automorphism of  $\Omega_1(P)$ .*

*Proof.* Clearly  $\Omega_1(P)$  is characteristic, so  $\alpha$  induces an automorphism of  $\Omega_1(P)$ . Let  $G = P \rtimes \langle \alpha \rangle$ . Suppose that  $\alpha$  fixes  $\Omega_1(P)$  pointwise. Let  $p^{i+1}$  be the exponent of  $P$ , and let  $x \in P$ . Then  $x^{p^i} \in \Omega_1(P)$ , so  $\alpha(x)x^{-1}$  has order dividing  $p^i$ , since

$$(\alpha(x)x^{-1})^{p^i} = \alpha(x^{p^i})(x^{p^i})^{-1} = 1.$$

In other words,  $[\langle \alpha \rangle, P] \leq \Omega_i(P)$  and hence  $[G, G, G] \leq \Omega_i(P)$  since  $G' \leq P$ . Repeating the argument, we see that  $G$  is nilpotent. But then  $G$  is the direct product of its Sylow subgroups, so  $\alpha$  centralises  $P$ .  $\square$

*Proof of Theorem 5.2.* Let  $G$  be a  $p'$ -embedding of  $S$ . In all cases we will obtain subgroups  $L_1, \dots, L_k$  of  $G$ , each belonging to one of the classes  $\mathcal{C}_{p'}^{\text{sep}}(S)$ ,  $\mathcal{C}_{p'}^{\text{LF}}(S)$  and  $\mathcal{C}_{p'}^{\text{L}}(S)$  (depending on whether  $E(G) = 1$  and/or  $G$  is  $p$ -separable), such that  $|G : S|$  is bounded by a function of  $\max |L_i : S|$  and  $S$ . The conclusion will then follow by Corollary 1.3.

Let  $P = O_p(G)$  and let  $P \leq F \leq G$  such that  $F/P = F^*(G/P)$ . Then the order of  $G/P$ , and thus the index  $|G : S|$ , is bounded by a function of  $|F : P|$ , since the generalised Fitting subgroup of  $G/P$  contains its own centraliser. In turn  $|F : P| = |F : O_p(F)|$  is bounded by a function of the  $p'$ -order of  $F$ , which is  $|FS : S|$ . Thus we may assume  $G = FS$ .

In this case  $G$  is the (permutable) product of the subgroups  $S, F_{p_1}, \dots, F_{p_m}, E_1, \dots, E_n$ , with  $p, p_1, \dots, p_m$  distinct primes, such that  $F_{p_i}/P = O_{p_i}(G/P)$  and  $E_j/P$  is the group generated by the  $S/P$ -conjugates of a component of  $G/P$ . Moreover,  $n$  is at most  $d(S)$  by Lemma 5.4.

Let  $H = SF_{p_i}$  for some  $i$ . Then  $H$  is prosoluble. Moreover, we have  $C_H(P) \leq P$ , because  $C_G(P)/Z(P)$  acts faithfully on  $E(G)$  by Lemma 2.4, whereas  $H$  centralises  $E(G)$ . Thus  $H \in \mathcal{E}_{p'}^{\text{sep}}(S)$ .

If  $G$  is prosoluble then  $n = 0$ . Otherwise let  $K = SE_j$  for some  $j$ . Since  $E_j$  is normal in  $G$  we have  $O_{p'}(E_j) = O_{p'}(G) = 1$ , so  $O_{p'}(K) = 1$ . Thus  $K \in \mathcal{E}_{p'}(S)$ . Also, any component of  $K$  is a component of  $E_j$  and hence of  $G$ , so if  $E(G) = 1$  then  $E(K) = 1$ .

Thus to obtain a bound on  $|G : S|$ , it suffices to bound the  $p'$ -order of each of the subgroups  $SF_{p_i}$  and  $SE_j$  individually.

Suppose  $G = SE_1$ . If  $E(G) > 1$ , then some and hence all components of  $G/P$  arise from components of  $G$ , that is  $G = SE(G)$ . Since the components of  $G/P$  form a single  $S$ -orbit, the same is true for the components of  $G$ , so  $G \in \mathcal{C}_{p'}^{\text{L}}(S)$ . Suppose instead that  $E(G) = 1$  and  $G$  is  $p$ -separable. Then by the Frattini argument, for each prime  $q$  dividing  $|E_1/P|$  we can find a  $q$ -Sylow subgroup  $H_q/P$  of  $E_1/P$  that is normalised by

$S/P$ , and then to bound the  $p'$ -order of  $G$ , it suffices to bound the  $p'$ -orders of the groups  $SH_q$  for all primes  $q$ . Note that as  $G$  is  $p$ -separable, we have  $E(G) = 1$ , ensuring that  $SH_q$  is a  $p'$ -embedding of  $S$  by Corollary 2.5. Thus this situation reduces to considering prosoluble  $p'$ -embeddings, which in turn reduces to  $p'$ -embeddings of the form  $G = SF_{p_i}$ .

The only remaining case of interest if  $G = SE_1$  is if  $E(G) = 1$  and  $p$  divides  $|E_1/P|$ , in which case  $G \in \mathcal{C}_{p'}^{\text{LF}}(S)$  by construction.

We have now reduced to the case  $G = SF_q$ , where  $q = p_1$  is some prime distinct from  $p$ .

Let  $\mathcal{N}$  be the class of  $p$ -separable  $p'$ -embeddings of  $S$  in which  $S$  is normal. If  $G \in \mathcal{N}$  then  $|G : S|$  divides  $|\text{GL}(d(S), p)|$ , so by Corollary 1.3,  $\mathcal{N}$  is finite. Let  $G \in \mathcal{E}_{p'}(S)$  and let  $R = O_p(G) \cap \Phi(S)$ . Suppose that  $G$  satisfies all the conditions for membership of the class  $\mathcal{C}_{p'}^{\text{ab}}(S)$ , except that  $N_G(R) \neq S$ . Then  $N_G(R) > S$ , so in fact  $N_G(R) = G$  by the irreducibility of the action of  $S$  on  $HP/P$ . Similarly, if  $G$  satisfies all the conditions for membership of the class  $\mathcal{C}_{p'}^{\text{crit}}(S)$  except that  $N_G(R) \not\leq \text{SZ}(H)$ , then  $R \trianglelefteq G$  by the irreducibility of the action of  $S$  on  $HP/Z(H)P$ . Thus  $G \in \mathcal{N}$  by Lemma 3.7. Write  $\mathcal{C}_{p'}^{\text{ab}}(S)' = \mathcal{C}_{p'}^{\text{ab}}(S) \cup \mathcal{N}$  and  $\mathcal{C}_{p'}^{\text{crit}}(S)' = \mathcal{C}_{p'}^{\text{crit}}(S) \cup \mathcal{N}$ .

Let  $H$  be a  $q$ -Sylow subgroup of  $G$  contained in  $F_q$ . Then  $H$  is a finite  $q$ -group and  $PH$  is normal in  $G$ . Our strategy is to bound  $|S : P|$ : this will produce a bound for  $|G : P|$ , because  $G/P$  acts faithfully on  $P/\Phi(P)$ , and by the Schreier index formula we have  $d(P) \leq |S : P|(d(S) - 1) + 1$ . Hence can freely replace  $G$  with a subgroup  $L$  of  $G$  containing  $S$  such that  $O_p(L) = P$ , or in other words  $L = SH_0$  where  $H_0$  is a subgroup of  $H$  such that  $S/P$  acts faithfully on  $H_0P/P$ . Thus we may assume  $G = O^q(G)$ , since  $O^q(G)$  is normal in  $G$  and contains  $S$ . By Theorem 2.7, we may assume  $H$  is critical in itself; otherwise we could replace  $H$  by a critical subgroup without changing  $O_p(G)$ . If  $H$  is abelian, we can replace  $H$  by  $\Omega_1(H)$ , by Lemma 5.5, and so assume  $H$  is elementary abelian.

Let  $M = HP/P$  if  $H$  is abelian and let  $M = HP/Z(H)P$  otherwise. Then  $M$  is a module for  $S$  over the field of  $q$  elements. By a version of Maschke's theorem,  $M$  is completely reducible.

Suppose  $H$  is abelian. Then we can write  $H = H_1 \times \cdots \times H_n$  such that for each  $i$ ,  $PH_i$  is a minimal normal subgroup of  $SH_i$ , and thus  $SH_i \in \mathcal{C}_{p'}^{\text{ab}}(S)'$ . Let  $P_i = O_p(SH_i)$ . Suppose now that  $\mathcal{C}_{p'}^{\text{ab}}(S)$  is finite. Then there are only finitely many possibilities for  $P_i$  as a subgroup of  $S$ ; thus there are only finitely many possibilities for  $P = \bigcap_{i=1}^n P_i$ . We see from this that there are only finitely many  $p'$ -embeddings of  $S$  of the form  $SK$  where  $K$  is abelian.

Suppose now that  $H$  is non-abelian. Then we can write  $H = H_1 \dots H_n$  such that  $H_i \cap H_j = Z(H)$  for  $i$  and  $j$  distinct, and so that  $PH_i/PZ(H)$  is a chief factor of  $SH_i$ . Again we set  $P_i = O_p(SH_i)$  and note that  $P = \bigcap_{i=1}^n H_i$ . If  $H_i$  is non-abelian, this implies  $SH_i \in \mathcal{C}_{p'}^{\text{crit}}(S)'$ , while if  $H_i$  is abelian, the finiteness of  $\mathcal{C}_{p'}^{\text{ab}}(S)$  leaves only finitely many possibilities for  $P_i$ . Thus if  $\mathcal{C}_{p'}^{\text{sep}}(S)$  is finite, there are only finitely many possibilities for

$P$  and hence for  $G$ .

The above argument shows that if  $\mathcal{C}_{p'}^{\text{sep}}(S)$ ,  $\mathcal{C}_{p'}^{\text{L}}(S)$  and  $\mathcal{C}_{p'}^{\text{LF}}(S)$  are all finite, then  $\mathcal{E}_{p'}(S)$  is finite. Note, moreover, that if  $G$  is in the class  $\mathcal{E}_{p'}^{\text{sep}}(S)$ , then  $|G : S|$  is in fact bounded using groups in  $\mathcal{C}_{p'}^{\text{sep}}(S)$  only, while if  $G$  is in the class  $\mathcal{E}_{p'}^{\text{LF}}(S)$ , the groups in  $\mathcal{C}_{p'}^{\text{sep}}(S) \cup \mathcal{C}_{p'}^{\text{LF}}(S)$  suffice. This demonstrates all three assertions in the theorem.  $\square$

## 6 Profinite groups with a cyclic or 2-generator Sylow subgroup

For this section,  $S$  is a pro- $p$  group such that  $d(S) \leq 2$ . The significance of this condition (in light of Lemma 3.7) is that if  $G$  is a  $p'$ -embedding of  $S$ , then either  $S/O_p(G)$  is cyclic, or else  $G$  is a Frattini  $p'$ -embedding and thus has a special structure.

First, consider the case that  $S$  is (topologically) cyclic, that is  $d(S) = 1$ . Here the possibilities are very straightforward:

**Proposition 6.1.** *Let  $S$  be a cyclic pro- $p$  group, and let  $G \in \mathcal{E}_{p'}(S)$ . Then exactly one of the following holds:*

- (i)  $S \trianglelefteq G$  and  $G/S$  is cyclic of order dividing  $p - 1$ ;
- (ii)  $S$  is finite and  $G$  has a single component  $Q$ , such that  $S \leq Q$  and  $G/Z(Q)$  is almost simple.

*Proof.* Let  $P = O_p(G)$ . If  $S = P$ , then case (i) occurs. Otherwise  $P \leq \Phi(S)$ , so  $G/P$  acts faithfully on  $E_p(G/P)$  by Lemma 3.7. Let  $R/P$  be a component of  $G/P$ . Then  $R$  is a central extension of  $P$  by  $R/P$ , since  $\text{Aut}(P)$  is  $p$ -separable, so there is a component  $Q$  of  $G$  such that  $R = PQ$ . Since  $Q \trianglelefteq G$  but  $Q$  is not  $p$ -separable, we have  $S \cap Q \not\leq \Phi(S)$  by Corollary 3.3, so  $S \leq Q$ . Clearly now  $Q = E_p(G) = E(G)$ , and  $G/Z(Q)$  is almost simple, since  $G/P = G/Z(Q)$  acts faithfully on  $Q/Z(Q)$ .  $\square$

We now obtain a list of possible structures for  $p'$ -embeddings of a 2-generator pro- $p$  group.

**Theorem 6.2.** *Let  $S$  be a pro- $p$  group such that  $d(S) = 2$ , and let  $G \in \mathcal{E}_{p'}(S)$ . Write  $P = O_p(G)$  and  $H = G/O_p(G)$ .*

*If  $G$  is a standard  $p'$ -embedding, then exactly one of the following holds:*

- (i)  $p$  is odd,  $S/P$  is non-trivial cyclic and there is a quasisimple normal subgroup  $Q$  of  $H$  such that  $S/P$  is a  $p$ -Sylow subgroup of  $Q$ ;

(ii)  $S/P$  is non-trivial cyclic,  $H$  acts faithfully on  $P/\Phi(P)$  and  $|F^*(H)|$  is coprime to  $p$ .

If  $G$  is a quasi-Frattini but not Frattini  $p'$ -embedding, then either (i) holds or the following holds:

(iii)  $S = P$  and  $H$  is isomorphic to a  $p'$ -subgroup of  $\mathrm{GL}(2, p)$ .

If instead  $G$  is a Frattini  $p'$ -embedding, then  $C_H(E_p(H)) = 1$  (so in particular  $E(H) = E_p(H)$ ) and exactly one of the following holds:

(iv) There is a subgroup  $Q$  of  $G$  containing  $S$  such that  $Q/P$  is a non-abelian simple group with a 2-generator  $p$ -Sylow subgroup;

(v)  $p$  is odd and there is a subgroup  $Q$  of  $G$  containing  $S$  such that  $Q/P$  is a direct product of two non-abelian finite simple groups (possibly isomorphic), each having a non-trivial cyclic  $p$ -Sylow subgroup;

(vi)  $E(H)$  is the direct product of  $p^l$  copies of a single non-abelian finite simple subgroup  $Q$  of  $H$  for some  $l \geq 0$ , with  $E(H)$  being the  $S$ -invariant closure of  $Q$ , and  $H/E(H)$  has a non-trivial cyclic  $p$ -Sylow subgroup.

*Proof.* Let  $k = |S : P\Phi(S)|$ . Since  $d(S) = 2$ , we have  $k \in \{1, p, p^2\}$ .

If  $k = 1$ , then  $S = P$  and we are clearly in case (iii) by Corollary 2.5. A  $p'$ -embedding with  $S = P$  is evidently quasi-Frattini but not Frattini.

If  $k = p$ , then  $S/P$  is non-trivial cyclic. If  $|F^*(H)|$  is coprime to  $p$ , we see that  $E(G) = 1$  since every component of  $G$  must have order divisible by  $p$ , so  $H$  acts faithfully on  $P/\Phi(P)$  by Corollary 2.5 and we are in case (ii). In case (ii),  $G$  is  $p$ -separable and therefore a standard  $p'$ -embedding by Lemma 3.7. If instead  $p$  divides  $F^*(H)$ , then there is some quasisimple subgroup  $Q$  of  $H$  of order divisible by  $p$ ; this ensures that  $|Q/Z(Q)|$  is also divisible by  $p$ . Let  $K$  be the normal closure of  $Q$  in  $H$ . Then  $K \geq S/P$ , since otherwise we would have  $K \cap S/P \leq \Phi(S/P)$ , which would imply that  $K$  has a normal  $p$ -complement by Corollary 3.3. Moreover,  $K$  is a central product of copies of  $Q$ ; since the  $p$ -Sylow subgroup of  $K$  is cyclic, there is only room for one copy of  $Q$ , in other words  $K = Q$ . We see that  $p$  is odd because there are no non-abelian finite simple groups with cyclic 2-Sylow subgroups (see for instance exercise 262 of [11]). Thus we are in case (i).

We may now assume  $k = p^2$ , in other words,  $G$  is a Frattini  $p'$ -embedding. We have  $C_H(E_p(H)) = 1$  by Lemma 3.7. To simplify notation, let us divide out by  $P$ ; in other words, assume that  $P = 1$  (so  $G = H$ ) and  $S$  is finite.

Suppose  $E_p(G) \geq S$ . By Corollary 3.3 applied to  $E_p(G)$ , every component  $Q$  of  $E_p(G)$  satisfies  $Q \cap S \not\leq \Phi(S)K$ , where  $K$  is the product of the other components. This leaves

only two possibilities: either  $E_p(G)$  is a non-abelian simple group  $Q$  with a 2-generator  $p$ -Sylow subgroup, or  $E_p(G) = Q_1 \times Q_2$ , where  $Q_1$  and  $Q_2$  are non-abelian simple groups with cyclic  $p$ -Sylow subgroups (here  $p$  is necessarily odd). These are cases (iv) and (v) respectively.

Finally, suppose  $E_p(G) \not\leq S$ . We cannot have  $E_p(G) \cap S \leq \Phi(S)$ , so  $\Phi(S)$  has index  $p$  in  $\Phi(S)(E_p(G) \cap S)$ . By Lemma 5.4, we see that  $E_p(G)$  is the  $S$ -invariant closure of a single component  $Q$ , in other words  $E_p(G)$  is the direct product of the  $S$ -conjugates of  $Q$ , whose number is a power of  $p$  as  $S$  is a pro- $p$  group. Since  $|S : \Phi(S)(E_p(G) \cap S)| = p$ , the  $p$ -Sylow subgroup of  $G/E_p(G)$  is non-trivial cyclic. This is case (vi).  $\square$

*Remark 1.* (a) Only cases (ii) and (iii) can give rise to  $p$ -separable  $p'$ -embeddings, and case (iii) accounts for only finitely many  $p'$ -embeddings. In cases (i), (iv) and (v), the isomorphism type of the simple group  $Q/Z(Q)$  involved in  $E(G/O_p(G))$  is restricted (see Lemma 7.3), while in each case a bound on the order of  $Q$  would imply a bound on the index  $|G : S|$ . Thus in cases (i), (iv) and (v), the possibility of infinitely many  $p'$ -embeddings remains only because of the existence of infinitely many finite simple groups of Lie type of small rank (obtained by varying the field of definition).

(b) If  $S$  is infinite and not finite-by- $\mathbb{Z}_p$ , then every finite normal subgroup of  $S$  is contained in  $\Phi(S)$ , so  $E(G) = 1$  for all  $p'$ -embeddings  $G$  of  $S$  by Corollary 3.3.

We now give a construction to demonstrate Proposition 1.5.

**Example 6.3.** Let  $p$  and  $q$  be primes. Let  $\mathbb{F} = \mathbb{F}_{p^q}$  and let  $\theta$  be the Frobenius automorphism of  $\mathbb{F}$ . Let  $K$  be the set of clopen subsets of  $\mathbb{Z}_p$ . Let  $F$  be the (elementary abelian) group of additive functions from  $K$  to  $\mathbb{F}$ , that is, functions  $f : K \rightarrow \mathbb{F}$  such that  $f(u \cup v) = f(u) + f(v)$  whenever  $u$  and  $v$  are disjoint. Let  $Z \cong \mathbb{Z}_p$  act on  $F$  by translating the elements of the domain, giving a semidirect product  $S = F \rtimes Z$ . We claim that  $S$  is a 2-generator metabelian pro- $p$  group; indeed it is the inverse limit of the 2-generator metabelian  $p$ -groups  $F_n \rtimes \mathbb{Z}_p/p^n\mathbb{Z}_p$ , where  $F_n$  is the group of functions from  $\mathbb{Z}_p/p^n\mathbb{Z}_p$  to  $\mathbb{F}$ . There is a natural surjective map  $\phi_n : F \rightarrow F_n$  formed by restricting the domain, and then maps  $F \rtimes \mathbb{Z}_p \rightarrow F_n \rtimes \mathbb{Z}_p/p^n\mathbb{Z}_p$  are given by extending  $\phi_n$  in a way that is compatible with the action of  $Z$  on  $F$ .

The group  $G$  is formed as  $F \rtimes (Q \rtimes Z)$ , equipped with the topology in which  $F \rtimes Z$  is an open compact subgroup, where  $Q$  is a subgroup of  $\text{Aut}(F)$  of the form  $\bigcup_{i \in \mathbb{N}} Q_i$ . As a group of automorphisms of  $F$ , the group  $Q_i$  has the following description:  $Q_i$  is a direct product of copies of  $C_q$  indexed by the elements of  $\mathbb{Z}_p/p^i\mathbb{Z}_p$ , and a generator for the  $j$ -th copy of  $C_q$  in  $Q_i$  acts on  $F$  by replacing  $f(u)$  by  $(f(u))^\theta$  for all  $f \in F$  and all  $u \in K$  such that  $u \subseteq j$ , with the consequent alteration of  $f(u)$  in the more general case that  $u \cap j \neq \emptyset$ . (Note that  $j$  is a coset of  $p^i\mathbb{Z}_p$ , being an element of  $\mathbb{Z}_p/p^i\mathbb{Z}_p$ ). It is easily verified that as subgroups of  $\text{Aut}(F)$ ,  $Q_i$  is normalised by  $Z$  and  $Q_i < Q_{i+1}$  for all  $i$ . Thus the groups

$$G_i = F \rtimes (Q_i \rtimes Z)$$



for  $i \geq 0$  form an ascending chain of subgroups of  $G$ , each open in the next, with union  $G$ . Given any finite image  $R$  of  $G_i$ , and given a conjugacy class  $C$  of  $R$ , then  $|C| = p^a q^b$  where  $b$  is at most  $p^i$ . Moreover, for a sufficiently large finite image, there is a conjugacy class contained in the image of  $F$  whose size is divisible by  $q^{p^i}$ : let  $\alpha \in \mathbb{F}$  be primitive, let  $f_i \in F$  be given by  $f_i(U) = |U \cap \{0, 1, \dots, p^i - 1\}| \alpha$ , and consider the conjugacy class of the image of  $f_i$  in a sufficiently large finite quotient of  $G_i$ . Thus the fusion of conjugacy classes of  $S$  in  $G_i$  and  $G_j$  is inequivalent for  $i \neq j$ , even up to automorphisms of  $S$ .

For  $p$  and  $q$  distinct primes, it is clear that this construction satisfies all assertions in Proposition 1.5.

In the construction, we notice totally disconnected, locally compact groups with a further interesting property. Let  $R = Q \rtimes Z \cong G/F$ . Let  $U$  be an open compact subgroup of  $R$ . We claim that  $N_R(U)/U$  is finite, and indeed that  $R$  acts properly by conjugation on the metric space of open compact subgroups of  $R$  with metric given by

$$d(U, V) = \log(|U : U \cap V| |V : U \cap V|).$$

To prove that the action on the above metric space is proper, it suffices to show that the set  $\{r \in R \mid |U : U \cap U^r| \leq p^k\}$  is compact for all  $k$  and fixed  $U$ , so we are free to take  $U = Z$ . In this case the set  $R_k = \{r \in R \mid |U : U \cap U^r| \leq p^k\}$  decomposes as  $R_k = (R_k \cap Q)Z$ . Now  $Z$  is compact, and  $R_k \cap Q$  is precisely the finite group  $C_Q(p^k U) = Q_k$ . Thus  $R_k$  is compact as required.

Note that the construction is valid even if  $p = q$ , in which case we obtain a metabelian totally disconnected, locally compact group  $R$  that is the union of an ascending chain of open pro- $p$  subgroups, such that every open compact subgroup of  $R$  has finite index in its normaliser.

## 7 Normal subgroup conditions

**Lemma 7.1.** *Let  $S$  be a finitely generated pro- $p$  group and let  $N$  be an open normal subgroup of  $S$ . Let  $\mathcal{K}$  be the set of open normal subgroups of  $S$  that are not contained in  $N$ . The following are equivalent:*

- (i)  $\mathcal{K}$  is finite;
- (ii)  $N$  contains every normal subgroup of  $S$  of infinite index.

*Proof.* Suppose there is a normal subgroup  $P$  of  $S$  of infinite index that is not contained in  $N$ . Then  $P$  is the intersection of a descending chain  $P_1 > P_2 > \dots$  of open normal subgroups of  $S$ , none of which are contained in  $N$ . Thus  $\mathcal{K}$  is infinite.

Conversely, suppose  $\mathcal{K}$  is infinite. We construct a directed graph  $\Gamma$  on  $\mathcal{K}$  by drawing an edge  $(K_1, K_2)$  if  $K_1 > K_2$  and  $K_1/K_2$  is a chief factor of  $S$ . Then every vertex lies on a path from the vertex  $S$ ; moreover,  $K/\Phi(K)$  is finite for every  $K \in \mathcal{K}$  since  $S$  is finitely generated, so  $\Gamma$  is locally finite. Thus  $\Gamma$  contains an infinite path by König's lemma, so there is an infinite descending chain  $L_1 > L_2 > \dots$  in  $\mathcal{K}$ . By a standard compactness argument, the intersection of the  $L_i$  is a normal subgroup  $L$  which is not contained in  $N$ , but  $L$  has infinite index.  $\square$

**Definition 7.2.** Let  $G$  be a finite simple group. Define  $\deg(G)$  to be the smallest number  $d$  such that  $G$  is isomorphic to a subgroup of  $\text{GL}(F^d)$  for some field  $F$ .

Given a profinite group  $G$  and a prime  $p$ , define  $d_p(G)$  to be  $d(S)$  where  $S$  is a  $p$ -Sylow subgroup of  $G$ .

**Lemma 7.3.** *Let  $p$  be a prime and let  $d$  be an integer. Then there some integer  $c$  depending on  $d$  and  $p$  such that if  $G$  is a finite simple group such that  $\deg(G) \geq c$ , then  $d_p(G) \geq d$ .*

*Proof.* See [10], section 1.7.  $\square$

*Proof of Theorem 1.6.* Let  $t$  be an integer such that  $d(S) - 1 \leq t$ , and also  $|S : K| \leq p^t$  for all  $K \in \mathcal{K}$ . By Lemma 7.1, every finite normal subgroup of  $S$  is contained in  $\Phi(S)$ . Thus  $\mathcal{E}_{p'}(S) = \mathcal{E}_{p'}^{\text{LF}}(S)$  by Corollary 3.4.

Let  $G$  be a  $p'$ -embedding of  $S$ , let  $P = \text{O}_p(G)$ , and let  $E$  be such that  $E/P = \text{E}_p(G/P)$ .

Suppose  $G$  is not a Frattini  $p'$ -embedding. Then  $P \in \mathcal{K}$ , so  $d(P) \leq tp^t + 1$  by the Schreier index formula. Since  $G/P$  acts faithfully on  $P/\Phi(P)$  (by Corollary 2.5), the index  $|G : P|$  is bounded, leaving only finitely many possibilities for  $G$  by Corollary 1.3. In particular, this accounts for all prosoluble  $p'$ -embeddings, so  $\mathcal{E}_{p'}^{\text{sep}}(S)$  is finite.

Now suppose  $|S : S^{(n)}|$  is finite for all  $n$ . By the previous argument, we may now assume  $G$  is a Frattini  $p'$ -embedding; this ensures that  $G/P$  acts faithfully on  $E/P$  by Lemma 3.7. We proceed by a series of claims.

(i) *We have  $d_p(Q) \leq tp^t + 1$  for every component  $Q$  of  $G/P$ .*

By Corollary 1.1, we have  $E \cap S \not\leq \Phi(S)$ , so  $E \cap S \in \mathcal{K}$ , and hence  $d(E \cap S) \leq tp^t + 1$  by the Schreier index formula; note that  $E \cap S$  is a  $p$ -Sylow subgroups of  $E$ . In turn, the direct decomposition of  $E/P$  ensures that  $d_p(Q) \leq d(E \cap S)$ .

(ii) *Let  $T$  be a  $p$ -Sylow subgroup of  $E/P$  contained in  $S/P$ . Then the derived length  $l$  of  $T$  is bounded by a function of  $p$  and  $t$ .*

Let  $Q$  be a simple direct factor of  $E/P$ . It follows from claim (i) and Lemma 7.3 that  $\deg(Q)$  is bounded by a function of  $p$  and  $t$ , so in particular  $Q$  has a faithful linear

representation of bounded degree. Thus, by a theorem of Zassenhaus ([18]), the derived length of any soluble subgroup of  $Q$  is bounded by a function of  $p$  and  $t$ . Since  $E/P$  is the direct product of its simple factors, the same bound applies to the derived length of  $T$ .

(iii) *There is a bound on  $|S : P|$  in terms of properties of  $S$ .*

Let  $R = S/P$ . We already know that  $|S : E \cap S|$  is at most  $p^t$ , so  $T$  contains  $R^{(t)}$ . But then  $R^{(t+l)} \leq T^{(l)} = 1$ , so  $S/P$  is soluble of derived length at most  $t + l$ . This means that  $P$  contains the open subgroup  $S^{(t+l)}$ , so  $|S : P|$  is bounded by properties of  $S$ .

(iv) *There is a bound on  $|G : P|$  in terms of properties of  $S$ .*

We have a bound on  $|S : P|$ , giving a bound on  $d(P)$  in terms of properties of  $S$ . But  $E(G) = 1$ , so  $G/P$  is isomorphic to a subgroup of  $\mathrm{GL}(d(P), p)$  by Corollary 2.5.

We conclude from claim (iv) and Corollary 1.3 that  $\mathcal{E}_{p'}(S)$  is finite.  $\square$

*Proof of Theorem 1.7.* Let  $\mathcal{K}$  be as in Theorem 1.6. Then  $\mathcal{K}$  is finite by Lemma 7.1. If  $S$  is insoluble, then  $\mathcal{E}_{p'}(S)$  is finite by Theorem 1.6. If  $S$  is soluble, then the last non-trivial term in its derived series has finite index, so  $S$  is virtually abelian. In this case  $S$  has finite subgroup rank  $r$  say. As a consequence, given any  $p'$ -embedding  $G$  of  $S$ , then  $G/O_p(G)$  is isomorphic to a subgroup of  $\mathrm{GL}(r, p)$  by Corollary 2.5 (since  $d(P) \leq r$  and  $E(G) = 1$ ), so  $|G : S|$  is bounded by a function of  $p$  and  $r$ , and thus  $\mathcal{E}_{p'}(S)$  is finite by Corollary 1.3.

For the final assertion, note that the just infinite groups  $G$  having  $S$  as a Sylow subgroup are precisely the  $p'$ -embeddings of  $S$ : since  $S$  is infinite, any just infinite profinite group  $G$  having  $S$  as a Sylow subgroup must have  $O_{p'}(G) = 1$ , and conversely any profinite group  $G$  with  $S$  as a Sylow subgroup and  $O_{p'}(G) = 1$  cannot have any finite normal subgroups, so  $G$  is just infinite by [8], Lemma 4.  $\square$

## 8 Weakly regular pro- $p$ groups

**Definition 8.1.** Let  $S$  be a finitely generated pro- $p$  group. Say  $S$  is *weakly regular* if there does not exist a surjective homomorphism  $S \rightarrow C_p \wr C_p$ .

**Theorem 8.2** (Yoshida [17] (finite version); Gilotti, Ribes, Serena [6] (profinite version)). *Let  $G$  be a profinite group and let  $S$  be a  $p$ -Sylow subgroup of  $G$ . Suppose  $S$  is weakly regular. Then  $N_G(S)$  controls  $p$ -transfer in  $G$ .*

As a consequence, we obtain significant restrictions on the structure of  $p'$ -embeddings of a weakly regular pro- $p$  group.

Given distinct primes  $p$  and  $q$ , write  $\text{ord}^\times(p, q)$  for the least positive integer  $a$  such that  $p^a \equiv 1 \pmod{q}$ . Note that the elementary abelian group of order  $p^d$  has an automorphism of order  $q$  if and only if  $\text{ord}^\times(p, q) \leq d$  (using the formula for the order of the general linear group).

**Theorem 8.3.** *Let  $S$  be a weakly regular pro- $p$  group and let  $G \in \mathcal{E}_{p'}(S)$ .*

- (i) *Suppose  $G$  is of the form  $G = SH$  where  $H$  is abelian and  $O_p(G)H$  is normal in  $G$ . Then  $S \trianglelefteq G$ . Consequently  $\mathcal{C}_{p'}^{\text{ab}}(S) = \emptyset$ .*
- (ii) *Let  $G \in \mathcal{E}_{p'}^{\text{sep}}(S)$  and let  $q$  be a prime divisor of  $|G : S|$ . Then  $S$  has an automorphism of order  $q$ , so in particular  $\text{ord}^\times(p, q) \leq d(S)$ . If  $q$  divides  $|G : N_G(S)|$ , then the following additional conditions are satisfied:*
  - (a)  *$S$  has an automorphism of order  $q$  that acts reducibly on  $S/\Phi(S)$ , so in particular  $\text{ord}^\times(p, q) < d(S)$ ;*
  - (b) *If  $p$  is odd, then  $\text{ord}^\times(q, p)$  is even.*
- (iii) *Let  $K$  be a normal subgroup of  $G$  such that  $K \leq S$ , and let  $Q/K$  be a component of  $G/K$  of order divisible by  $p$ . Then  $S$  normalises  $Q$ . In particular, if  $G \in \mathcal{C}_{p'}^{\text{LF}}(S) \cup \mathcal{C}_{p'}^{\text{L}}(S)$ , then  $G$  has exactly one non-abelian composition factor.*

Theorem 8.3 will be proved at the end of this section.

**Example 8.4.** Given  $d(S)$  and  $p$ , let  $\pi$  be the set of primes satisfying the conditions in Theorem 8.3 (ii). For some values of  $d(S)$  and  $p$ , the set  $\pi$  is surprisingly small. For instance, suppose  $p = 3$ , and  $d(S) \leq 11$ . Then  $\pi = \{2, 5, 11, 41\}$ . So if  $S$  is a weakly regular pro-3 group generated by at most 11 elements, and  $G$  is a 3-separable 3'-embedding of  $S$ , then the prime divisors of  $|G : N_G(S)|$  are a subset of  $\{2, 5, 11, 41\}$ . Similarly, if  $p = 7$  and  $d(S) \leq 8$ , then  $\pi \subseteq \{3, 5, 19\}$ .

**Lemma 8.5.** *Let  $S$  be a pro- $p$  group and let  $G \in \mathcal{E}_{p'}^{\text{LF}}(S)$ . Let  $K$  be a subgroup of  $G$  that properly contains  $S$ .*

- (i)  *$S$  does not control  $p$ -transfer in  $K$ .*
- (ii) *Suppose  $S$  is weakly regular. Then  $N_K(S) > S$ .*

*Proof.* (i) Suppose  $S$  controls  $p$ -transfer in  $K$ . Then by Theorem 3.2,  $O^p(K) = O_{p'}(K)$  is a complement to  $S$  in  $K$ . But by Corollary 2.5  $O_{p'}(K) = 1$ , so  $K$  is a pro- $p$  group, which is impossible since  $S$  is a maximal pro- $p$  subgroup of  $G$ .

(ii) This follows immediately from part (i) together with Theorem 8.2.  $\square$

**Proposition 8.6.** *Let  $S$  be a weakly regular pro- $p$  group, and let  $G \in \mathcal{E}_{p'}^{\text{LF}}(S)$ . Let  $H = S[G, S]$ , and let  $P = O_p(G)$ . Then:*

- (i) Any abelian  $p'$ -subgroup of  $G/P$  that is normalised by  $H/P$  is centralised by  $H/P$ ;
- (ii)  $F(H/P)$  has nilpotency class at most 2.

*Proof.* (i) It suffices to consider abelian  $q$ -subgroups of  $G/P$ , where  $q \in p'$ . Let  $K \leq G$  such that  $K'O^q(K) \leq O_p(G)$  and  $[K, H] \leq O_p(G)K$ ; it is clear that this accounts for all abelian  $q$ -subgroups of  $G/P$  that are normalised by  $H/P$ . Then  $N_{K/P}(S/P) = C_{K/P}(S/P)$ , and  $[K/P, S/P] \cap C_{K/P}(S/P) = 1$  by part (iii) of Lemma 2.3. Let  $M = S[K, S]$ . Since  $P \leq S$ , it follows that  $N_M(S) = S$ . Hence  $M = S$  by Lemma 8.5, so  $[K, S] \leq K \cap S \leq P$ . The same argument shows that  $K/P$  commutes with every  $p$ -Sylow subgroup of  $G/P$ . But  $H/P$  is generated by these  $p$ -Sylow subgroups by construction, so  $K/P$  is centralised by  $H/P$ .

(ii) Write  $T = F(H/P)$ . Since  $H/P$  is finite,  $T$  is nilpotent. Let  $c$  be the nilpotency class of  $T$ , and assume  $c > 2$ . Then  $\gamma_{c-1}(T)$  is abelian, since  $[\gamma_{c-1}(T), \gamma_{c-1}(T)] \leq \gamma_{2c-2}(T)$ , and  $2c-2 = c + (c-2) > c$ ; thus  $\gamma_{c-1}(T)$  is central in  $T$  by part (i). But then  $\gamma_c(T) = 1$ , contradicting the definition of  $c$ .  $\square$

**Corollary 8.7.** *Let  $S$  be a weakly regular pro- $p$  group, and let  $G$  be a prosoluble  $p'$ -embedding of  $S$ . Let  $H = S[G, S]$ , and let  $P = O_p(H)$ . Then either  $G$  is  $p$ -normal, or  $F(H/P)$  has nilpotency class exactly 2.*

*Proof.* By Proposition 8.6,  $F(H/P)$  has nilpotency class at most 2, and clearly  $H = P$  if  $G$  is  $p$ -normal; hence we may assume  $F(H/P)$  has nilpotency class less than 2. This means  $F(H/P)$  is abelian, and so by the proposition  $F(H/P) = Z(H/P)$ . Now  $H/P$  is a finite soluble group, so  $F(H/P) \geq C_{H/P}(F(H/P)) = H/P$ , so  $H/P$  is abelian, which means  $S$  is normal in  $H$ . By Sylow's theorem,  $S$  is the unique  $p$ -Sylow subgroup of  $H$ . But  $H$  is generated by its  $p$ -Sylow subgroups. Hence  $H = S$ , which means that  $G$  is  $p$ -normal.  $\square$

**Lemma 8.8.** *Let  $p$  be a prime, and let  $q$  be a prime power coprime to  $p$ . Let  $n$  be any positive integer. Suppose  $p$  is odd, and let  $G = \mathrm{Sp}(2n, q)$ , considered as a subgroup of  $\mathrm{GL}(V)$  where  $V = \mathbb{F}_q^{2n}$ . Suppose a  $p$ -Sylow subgroup of  $G$  acts irreducibly on  $V$ . Then  $\mathrm{ord}^\times(q, p)$  is even.*

*Proof.* See Table 1 of [13]. The Sylow subgroups of 'type B' in this table are necessarily reducible.  $\square$

**Lemma 8.9.** *Let  $q$  be an odd prime, and let  $U$  be a  $q$ -group of nilpotency class 2. Let  $P$  be a  $p$ -group of automorphisms of  $U$ , where  $p \neq q$ , such that  $P$  centralises  $Z(U)$ . Suppose also that  $M = U/Z(U)$  is irreducible as a  $P$ -module. Let  $N$  be a maximal subgroup of  $U'$ , and identify  $U'/N$  with  $\mathbb{F}_q$ . Then the homomorphism  $(-, -)_N$  from  $M \times M$  to  $U'/N$  defined by  $(xZ(U), yZ(U))_N = [x, y]N$  is a non-degenerate, skew-symmetric, alternating bilinear form for  $M$  as a vector space over  $\mathbb{F}_q$ , and this form is preserved by  $P$ . Hence  $P$*

acts on  $M$  as a subgroup of  $\mathrm{Sp}(M)$ , the symplectic group on  $M$  associated to the given form. In particular,  $p \cdot \mathrm{ord}^\times(q, p)$  is even.

*Proof.* The equation  $(xZ(U), yZ(U))_1 = [x, y]$  specifies a function  $(-, -)_1$  from  $M \times M$  to  $U'$ . This is a homomorphism since  $M$  is abelian, and hence it is surjective by the definition of  $U'$ ; hence  $(-, -)_N$  is a non-trivial quadratic form. The form is preserved by  $P$  since  $P$  centralises  $Z(U)$ , which contains  $U'$ , and  $M$  is irreducible as a  $P$ -module, so  $(-, -)_N$  is non-degenerate on  $M$ . Finally,  $(-, -)_N$  is also skew-symmetric and alternating, since  $[x, y] = [y, x]^{-1}$  and  $[x, x] = 1$  are identities in any group.

We conclude that  $P$  acts on  $M$  as a subgroup of  $\mathrm{Sp}(M)$ . Hence  $\mathrm{Sp}(M)$  has a non-trivial irreducible  $p$ -subgroup. This implies at least one of  $p$  and  $\mathrm{ord}^\times(q, p)$  is even, by Lemma 8.8.  $\square$

*Proof of Theorem 8.3.* (i) Let  $P = \mathrm{O}_p(G)$ . In this case, we see from Proposition 8.6 that  $HP/P$  is central in  $S[G, S]/P$ , which implies that  $S$  is normal in  $S[G, S]$ . Since  $S[G, S]$  is normal in  $G$ , it follows by Sylow's theorem that  $S$  is normal in  $G$ .

(ii) Let  $q$  be a prime divisor of  $|G : S|$ . Then  $q$  divides at least one of  $|G : \mathrm{N}_G(S)|$  and  $|\mathrm{N}_G(S) : S|$ . If  $q$  divides  $|\mathrm{N}_G(S) : S|$ , then there is an automorphism of  $S$  of order  $q$  induced by conjugation in  $\mathrm{N}_G(S)$ , since  $\mathrm{C}_G(S) \leq S$ , and hence  $\mathrm{ord}^\times(p, q) \leq d(S)$  by Lemma 2.3. So from now on we may assume  $q$  divides  $|G : \mathrm{N}_G(S)|$ .

Let  $G_0 = 1$  and thereafter let  $G_{i+1}$  be such that  $G_{i+1}/G_i = \mathrm{O}_p(G/G_i) \times \mathrm{O}_{p'}(G/G_i)$ . We obtain a series

$$G_1 < \cdots < G_n = G$$

of open normal subgroups of  $G$ , where for all  $i \geq 0$ , the quotient  $G_{i+1}/G_i$  is a pro- $p$  group if  $i$  is even and a  $p'$ -group if  $i$  is odd. Set  $H_i = G_{2i+1}$ . By the Frattini argument, for each index  $i$  there is a  $q$ -Sylow subgroup  $T_i/H_i$  of  $\mathrm{O}_{p'}(G/H_i)$  that is normalised by  $S$ . The condition that  $q$  divides  $|G : \mathrm{N}_G(S)|$  ensures that there is some  $j \geq 0$  such that  $S$  does not centralise  $T_j/H_j$ . Now let  $R = SG_{2j}/G_{2j}$  and consider the group  $H = ST_j/G_{2j}$ . We see that  $G/G_{2j} \in \mathcal{E}_{p'}^{\mathrm{LF}}(R)$ , so by Corollary 2.5 we have  $H \in \mathcal{E}_{p'}^{\mathrm{LF}}(R)$ ; indeed  $H \in \mathcal{E}_{p'}^{\mathrm{sep}}(R)$  since  $H$  is  $p$ -separable. Moreover,  $R$  is weakly regular and  $q$  divides  $|R : \mathrm{N}_H(R)|$ , since  $R$  does not normalise  $S$ . Thus we may assume  $G = ST$ , where  $T$  is a finite  $q$ -group, and that  $T\mathrm{O}_p(G)/\mathrm{O}_p(G)$  is normal in  $G/\mathrm{O}_p(G)$ . Indeed, by Theorem 2.7, we can find a characteristic critical subgroup  $U$  of  $T$  such that  $S$  does not centralise  $U$ , and replacing  $G$  with  $S[G, S] = \mathrm{O}^q(G)$  has no effect on the prime divisors of  $|G : \mathrm{N}_G(S)|$ , since  $G = S[G, S]\mathrm{N}_G(S)$  by the Frattini argument. The case  $G \in \mathcal{C}_{p'}^{\mathrm{ab}}(S)$  was already eliminated in part (i). So we may assume  $T$  is non-abelian, with no proper critical subgroups, so  $T/\mathrm{Z}(T)$  is elementary abelian. Furthermore, we can replace  $T$  with a subgroup  $U > \mathrm{Z}(T)$  such that  $U\mathrm{O}_p(G)/\mathrm{Z}(T)\mathrm{O}_p(G)$  is a chief factor of  $G$ , and then  $\mathrm{Z}(U) = \mathrm{Z}(T)$  by Proposition 8.6. Thus we may assume  $G \in \mathcal{C}_{p'}^{\mathrm{crit}}(S)$ .

Let  $L = N_G(S)$ . Since  $O^p(G) \cap S > 1$ , we have  $O^p(L) \cap S > 1$  by Theorem 8.2 and Theorem 3.2. Applying Theorem 3.2 again we see that  $L'L^p \cap S \neq \Phi(S)$ , which means that  $L$  acts non-trivially on  $S/\Phi(S)$ . At the same time, the action of  $L$  on  $S/\Phi(S)$  is reducible, since there is a proper non-trivial invariant subspace  $O_p(G)\Phi(S)/\Phi(S)$ : we have  $O_p(G) < S$  since  $S$  is not normal in  $G$ , so  $O_p(G)\Phi(S) < S$  by the fact that  $\Phi(S)$  is the intersection of all maximal closed subgroups of  $S$ , and we have  $O_p(G) \not\leq \Phi(S)$  by Corollary 3.3. This establishes condition (a).

For condition (b), let  $U = TO_p(G)/O_p(G) = F(G/O_p(G))$ . Note that  $Z(U)$  is central in  $G/O_p(G)$  by Proposition 8.6, and  $U/Z(U)$  is a chief factor of  $G/O_p(G)$  since  $G \in \mathcal{C}_{p'}^{\text{crit}}(S)$ . We are now in the situation of Lemma 8.9, and so  $p \cdot \text{ord}^\times(q, p)$  is even.

(iii) Let  $R$  be the product of all  $S$ -conjugates of  $Q$  and let  $C = C_{SR}(R)$ . Then  $SR/C$  is a  $p'$ -embedding of  $SC/C$ , so we may assume  $G = SR$  and  $C_G(R) = 1$ . Moreover,  $R$  is of the form  $Q_1 \times \cdots \times Q_n$  where  $Q_i$  is an  $S$ -conjugate of  $Q$ . Notice that  $N_R(S)$  decomposes as

$$N_{Q_1}(S_1) \times \cdots \times N_{Q_n}(S_n),$$

where  $S_i = S \cap Q_i$ . We have  $N_{SR}(S) > S$  by Lemma 8.5, so  $N_{Q_i}(S) > S_i$  for some  $i$ ; hence  $N_Q(S) > S$ . Thus there is some element  $x \in N_Q(S)$  of order  $q$ , where  $q$  is a prime distinct from  $p$ . Suppose that  $S$  does not normalise  $Q$ ; let  $y \in S \setminus N_S(Q)$ . Then  $x$  and  $xyx^{-1}$  lie in distinct factors  $Q_i$ , so  $z = xyx^{-1}y^{-1}$  has order  $q$ . But  $z$  is contained in  $[S, N_Q(S)] \leq S$ , so  $z$  is contained in a pro- $p$  group, a contradiction.  $\square$

## Acknowledgements

This paper is based on results obtained by the author as a PhD student at Queen Mary, University of London under the supervision of Robert Wilson, supported by EPSRC. I would also like to thank Charles Leedham-Green for his advice and guidance during my doctoral studies.

## References

- [1] M. Aschbacher, *Finite Group Theory*, CUP 2000.
- [2] D. A. Craven, *Fusion Systems: An Algebraic Approach*, CUP 2011.
- [3] L. Evens, *The Cohomology of Groups*, OUP, New York, 1991.
- [4] W. Feit, J. G. Thompson, Solvability of groups of odd order, *Pacific J. Math.* 13 (1963), 775–1029.
- [5] S. M. Gagola Jr., I. M. Isaacs, Transfer and Tate’s theorem, *Arch. Math. (Basel)* 91 (2008), no. 4, 300–306.

- [6] A. L. Gilotti, L. Ribes, L. Serena, Fusion in Profinite Groups, *Annali di Matematica pura ed applicata* (4), 177 (1999), 349–362.
- [7] C. R. Leedham-Green, S. McKay, *The Structure of Groups of Prime Power Order*, OUP, New York, 2002.
- [8] C. D. Reid, Subgroups of finite index and the just infinite property, *J. Alg.* 324 (2010), 2219–2222.
- [9] C. D. Reid, The generalized pro-Fitting subgroup of a profinite group, to appear in *Comm. Alg.*
- [10] C. D. Reid, Finiteness Properties of Profinite Groups, PhD thesis, University of London 2010. arXiv:1002.2935v1
- [11] J. S. Rose, *A Course on Group Theory*, Dover 1978.
- [12] R. Stancu, P. Symonds, Fusion Systems for Profinite Groups, preprint 2012, <http://www.maths.manchester.ac.uk/~pas/preprints/profusionsystems.pdf>
- [13] M. Stather, Constructive Sylow theorems for the classical groups, *J. Algebra* 316 (2007), no. 2, 536–559.
- [14] P. Symonds, On cohomology isomorphisms of groups, *J. Algebra* 313 (2007), no. 2, 802–810.
- [15] J. Tate, Nilpotent quotient groups, *Topology* 3 (1964) suppl. 1, 109–111.
- [16] J. S. Wilson, *Profinite groups*, Clarendon Press, Oxford, 1998.
- [17] T. Yoshida, Character-theoretic Transfer, *J. Algebra*, 52 (1978), 1–38.
- [18] H. Zassenhaus, Beweis eines Satzes über diskrete Gruppen, *Abh. Math. Sem. Univ. Hamburg* 12 (1938), 289–312.